Discrete Mathematics 106/107 (1992) 147–155
North-Holland

On the covering radius of Reed–Muller codes

Gérard D. Cohen

Ecole Nationale Supérieure des Télécommunications, Département Informatique, 46 Rue Barrault, 75634 Paris Cedex 13, France

Simon N. Litsyn*

Tel Aviv University, Department Electrical Engineering-Systems, 69978 Ramat Aviv, Israel

Received 4 November 1991
Revised 14 January 1992

Abstract

Cohen, G.D., S.N. Litsyn, On the covering radius of Reed–Muller codes, Discrete Mathematics 106/107 (1992) 147–155.

We present lower and upper bounds on the covering radius of Reed–Muller codes, yielding asymptotical improvements on known results. The lower bound is simply the sphere covering one (not very new). The upper bound is derived from a thorough use of a lemma, the 'essence of Reed–Mullerity'. The idea is to find a 'seed' upper bound—a properly chosen combination of binomial coefficients—well fitted to the respective growths of m (log of length) and r (order), to initiate double induction on m and r. Surprisingly enough, these two simple ingredients suffice to essentially fill the gaps between lower and upper bounds, a result stated in our theorem.

1. Introduction

We present lower and upper bounds on the covering radius of Reed–Muller codes, yielding asymptotical improvements on known results (see for example [4, 5]). The lower bound is simply the sphere covering one (not very new). The upper bound is derived from a thorough use of a lemma, the 'essence of Reed–Mullerity'. The idea is to find a 'seed' upper bound—a properly chosen combination of binomial coefficients—well fitted to the respective growths of m (log of length) and r (order), to initiate double induction on m and r. Surprisingly enough, these two simple ingredients suffice to essentially fill the gaps between lower and upper bounds, a result stated in our theorem.

Correspondence to: G. Cohen, Ecole Nationale Supérieure des Télécommunications, Département Informatique, 46 Rue Barrault, 75634 Paris Cedex 13, France.

* This work was done while S.N. Litsyn was visiting Department Informatique, ENST during summer 1991.

As is well known (see, e.g., [3]), $R(r, m)$, the rth order Reed–Muller code has length $n = 2^m$, dimension $k = \sum_{i=0}^{r} \binom{m}{i}$ and minimum distance $d = 2^{m-r}$. We denote by $\rho(r, m)$ or simply ρ its covering radius (see [1]) and deal with asymptotical lower and upper estimates of it when $m \to \infty$. The entropy function is $H(x) := -x \log x - (1-x)\log(1-x)$, where log is binary.

2. Lower bounds

We use the classical sphere-covering bound:

$$k(r, m) + \log \sum_{i=0}^{\rho} \binom{2^m}{i} \geq 2^m. \tag{0}$$

Case 1: $m - r = o(m)$.

We write (0) as

$$\log \sum_{i=0}^{\rho} \binom{2^m}{i} \geq \sum_{i=0}^{m-r-1} \binom{m}{i}.$$

Now, combining (a) and (b), where

(a) $$\sum_{i=0}^{m-r-1} \binom{m}{i} \geq \frac{m^{m-r-1}}{(m-r-1)!};$$

(b) $$\log \sum_{i=0}^{\rho} \binom{2^m}{i} \leq \log \rho + m\rho - \log \rho = m\rho;$$

we get

$$\rho(r, m) \geq \frac{m^{m-r-2}}{(m-r-1)!}. \tag{1}$$

Case 2: $r = o(m)$.

Here (0) gives

$$\log \sum_{i=0}^{\rho} \binom{2^m}{i} \geq 2^m - \sum_{i=0}^{r} \binom{m}{i}.$$

(a) $$2^m - \sum_{i=0}^{r} \binom{m}{i} \geq 2^m - m^r/r!;$$

(b) $$\log \sum_{i=0}^{\rho} \binom{n}{i} \leq \log \rho + nH(\rho/n).$$

Setting $x := 2^{m-1} - \rho$, $y := x/n$ and taking into account $H(\frac{1}{2} - y) \approx 1 - 2y^2$ for $y \to 0$, we get

$$\rho \geq 2^{m-1} - 2^{m/2} m^{r/2} ((\ln 2)/2r!)^{\frac{1}{2}}. \tag{2}$$

Case 3: $r/m =: \alpha > \frac{1}{2}$.
In this case $\rho \ll n$,

(a) $$\log \sum_{i=0}^{\rho} \binom{n}{i} \lesssim m\rho;$$

(b) $$\sum_{i=0}^{m-r-1} \binom{m}{i} \gtrsim \frac{1}{2\sqrt{2m\alpha(1-\alpha)}} 2^{mH(1-\alpha)};$$

and

$$\rho \gtrsim (2m^3)^{-\frac{1}{2}} 2^{mH(\alpha)}. \tag{3}$$

Case 4: $\alpha < \frac{1}{2}$.
In this case $x = 2^{m-1} - \rho \ll 2^m$.

(a) $$\log \sum_{i=0}^{\rho} \binom{n}{i} \lesssim n - 2x^2/(n \ln 2);$$

(b) $$\sum_{i=0}^{m-r-1} \binom{m}{i} = 2^m - \sum_{i=0}^{r} \binom{m}{i} \gtrsim 2^m - 2^{mH(\alpha)};$$

and

$$\rho \gtrsim 2^{m-1} - ((\ln 2)/2)^{\frac{1}{2}} 2^{m(1+H(\alpha))/2}. \tag{4}$$

3. Upper bounds

The following result is simple but essential to our purpose.

Lemma. $\rho(r, m) \leq \rho(r-1, m-1) + \rho(r, m-1)$.

Proof. Reed–Muller codes are inductively defined (see [3]) by $R(r, m) = \{(u, u+v)\colon\ u \in R(r, m-1),\ v \in R(r-1, m-1)\}$; where $(\cdot, \cdot)$ denotes concatenation. Let $x = (x_1, x_2)$ be an arbitrary vector, then x can be 'approximated' by first choosing u, a closest word to x_1 in $R(r, m-1)$, and then v, a closest word to $x_2 + u$ in $R(r-1, m-1)$. Then

$$\begin{aligned} d((x_1, x_2), (u, u+v)) &= d(x_1, u) + d(x_2, u+v) \\ &\leq \rho(r, m-1) + \rho(r-1, m-1). \end{aligned}$$ □

Case 1: $m - r = \lambda = o(m)$.
We prove by induction on λ,

$$\rho(r, m) \lesssim \frac{m^{m-r-2}}{(m-r-2)!} + O(m^{m-r-3}). \tag{5}$$

The inequality is valid for $\lambda = 3$ (see [2]). Let it be valid for $(m-r-1)$. Then

$$\begin{aligned}\rho(r, m) &\leqslant \rho(r-1, m-1) + \rho(r, m-1)\\ &\leqslant \rho(r-1, m-1) + \frac{(m-1)^{m-r-3}}{(m-r-3)!} + O(m^{m-r-4})\\ &\leqslant \sum_{i=1}^{r} \frac{(m-i)^{m-r-3}}{(m-r-3)!} + \sum_{i=1}^{r} O(m^{m-r-4})\\ &\quad + \rho(0, m-r) \leqslant \frac{m^{m-r-2}}{(m-r-2)!} + O(m^{m-r-3}).\end{aligned}$$

Case 2: $r = o(m)$.

We prove by induction that for $r \geqslant 2$

$$\rho(r, m) \leqslant 2^{m-1} - (\sqrt{2}+1)^{r-1} 2^{(m-2)/2} + O(m^{r-2}). \tag{6}$$

Using results on upper bounds for $\rho(1, m)$ we have

$$\begin{aligned}\rho(2, m) &\leqslant \rho(2, m-1) + \rho(1, m-1) \leqslant \rho(2, m-1) + 2^{m-2} - 2^{(m-3)/2}\\ &\leqslant \rho(2, 2) + \sum_{i=1}^{m-2} 2^i - \sum_{i=0}^{m-3} 2^{i/2} \leqslant 2^{m-1} - (\sqrt{2}+1)2^{(m-2)/2}.\end{aligned}$$

Let (6) be valid for $r-1$. Then

$$\begin{aligned}\rho(r, m) &\leqslant \rho(r, m-1) + \rho(r-1, m-1)\\ &\leqslant \rho(r, m-1) + 2^{m-2} - 2^{(m-3)/2}(\sqrt{2}+1)^{r-2} + O(m^{r-3})\\ &\leqslant \rho(r, r) + \sum_{i=r}^{m-2} 2^i - (\sqrt{2}+1)/3)^{r-2} \sum_{i=r-3}^{m-3} 2^{i/2} + O(m^{r-2})\\ &\leqslant 2^{m-1} - 2^{(m-2)/2}(\sqrt{2}+1)^{r-1}.\end{aligned}$$

Let us compare our bound with one from [4],

$$\rho(r, m) \leqslant 2^{m-1} - (2^{r/2} - 2^{r/6})(2^m - 2^r)^{\frac{1}{2}}$$

For $r = \text{const}$, this gives $\rho(r, m) \leqslant 2^{m-1} - (2^{r/2} - 2^{r/6})2^{m/2}$. We have in this range $\rho(r, m) \leqslant 2^{m-1} - \frac{1}{2}(2.42)^{r-1}$. For example, for $r = 2$, [4] and (6) yield respectively

$$\rho(2, m) \leqslant 2^{m-1} - 0.74\ldots 2^{m/2},$$

$$\rho(2, m) \leqslant 2^{m-1} - 1.21\ldots 2^{m/2}.$$

Case 3: $\alpha = r/m = \text{const} > \frac{1}{2}$.

We prove by induction that for $r \leqslant m-3$

$$\rho(r, m) \leqslant \sum_{i=1}^{m-r-2} \binom{m+2}{i}.$$

The inequality holds for $r = m-3$, as well as it is valid for $r = 0$. Let it be valid

for $(m-r-1)$ and all m, and for $(m-r)$ and all lengths less than 2^m. Then,

$$\rho(r, m) \leqslant \sum_{i=1}^{m-r-2} \binom{m+1}{i} + \sum_{i=1}^{m-r-3} \binom{m+1}{i}$$
$$= \sum_{i=1}^{m-r-2} \binom{m+2}{i} - 1 < \sum_{i=1}^{m-r-2} \binom{m+2}{i}.$$

Standard arguments give

$$\rho(r, m) \lesssim 2^{nH(1-\alpha)}. \tag{7}$$

Case 4: $\alpha = r/m = \text{const} < \frac{1}{2}$.

We prove by induction that for $r \geqslant 1$

$$\rho(r, m) \leqslant 2^{m-1} - \binom{m}{r}.$$

The inequality holds for $r = 1$ and all m, and for $r = m$ and all r. Let it be valid for $r-1$ and all m, and for r and $m-1$. Then,

$$\rho(r, m) \leqslant 2^{m-2} - \binom{m-1}{r} + 2^{m-2} - \binom{m-1}{r-1} = 2^{m-1} - \binom{m}{r}.$$

This gives asymptotically

$$\rho(r, m) \lesssim 2^{m-1} - 2^{mH(\alpha)}(2m\alpha(1-\alpha))^{-\frac{1}{2}}. \tag{8}$$

For $0 \leqslant r/m \leqslant (2+\sqrt{2})^{-1}$, the following inequality holds:

$$\rho(r, m) \leqslant 2^{m-1} - (\sqrt{2}+1)^{r-1} 2^{(m-2)/2} + r\binom{m}{r}. \tag{9}$$

The proof by induction is quite technical and is presented as an appendix. Denoting $\rho(r, m) = 2^{m-1} - 2^{mf(\alpha)}$ and combining (3), (9) and (8) gives the following.

$$\tfrac{1}{2}(1+H(\alpha)) \gtrsim f(\alpha) \geqslant \begin{cases} \frac{1}{2} + \alpha \log 2(\sqrt{2}+1), & 0 \leqslant \alpha \leqslant 1 - \sqrt{2}/2 \approx 0.293, \\ H(\alpha), & 1 - \sqrt{2}/2 \leqslant \alpha \leqslant \frac{1}{2}. \end{cases}$$

This corresponds to the dotted area in Fig. 1.

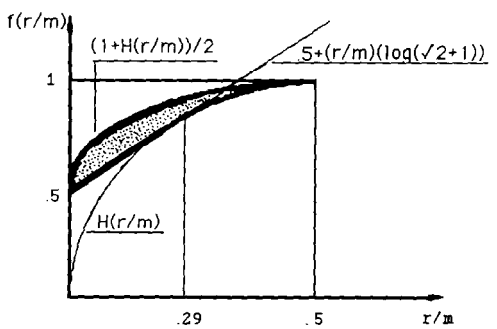

Fig. 1. Bounds for $r/m < 0.5$.

When r/m grows from 0 to 1, the rate $R = k/m$ of $R(r, m)$ grows from 0 to 1. Asymptotically the behavior is discontinuous, with

$$R = 0 \text{ for } r/m < \tfrac{1}{2},$$

$$R = 1 \text{ for } r/m > \tfrac{1}{2},$$

and

$$R = \tfrac{1}{2} \text{ for } r/m = \tfrac{1}{2}.$$

We shall now treat this last case.

A lower bound on ρ is readily obtained through the sphere covering bound, yielding

$$\rho \gtrsim nH^{-1}(\tfrac{1}{2}). \tag{10}$$

For the upper bound, we use a result from [4]: If h is a positive integer such that $m - 2 \geq r \geq (h-1)(m-1)/h$, then

$$\rho(r, m) \leq 2^{m-h} - 2^{r+2-h} + 2.$$

For $h = 2$, this gives

$$\rho(m/2, m) \leq 2^{m-2} - 2^{m/2} + 2 \lesssim (\tfrac{1}{4})n. \tag{11}$$

Summarizing (1)–(11), we have the following.

Theorem. *For m large enough, if $o(m) = m - r \geq 3$, then*

$$\frac{m^{m-r-2}}{(m-r-1)!} \lesssim \rho(r, m) \lesssim \frac{m^{m-r-2}}{(m-r-2)!},$$

i.e., $\rho(r, m) = \theta(m^{m-r-2})$. If $r \geq 2$, $r = o(m)$, then

$$2^{m-1} - 2^{m/2} m^{r/2} ((\ln 2)/2r!)^{\frac{1}{2}} \lesssim \rho(r, m) \lesssim 2^{m-1} - 2^{m/2}(\sqrt{2}+1)^{r-1}.$$

If $r/m = \text{const}$, $r/m \geq \frac{1}{2}$, then

$$(2m^3)^{-\frac{1}{2}} 2^{mH(1-r/m)} \lesssim \rho(r, m) \lesssim 2^{mH(1-r/m)}.$$

If $(2+\sqrt{2})^{-1} \lesssim r/m \lesssim \frac{1}{2}$, then

$$2^{m-1} - ((\ln 2)/2)^{\frac{1}{2}} 2^{m(1+H(r/m))/2} \lesssim \rho(r, m) \lesssim 2^{m-1} - 2^{mH(r/m)}.$$

If $0 \leq r/m \leq (2+\sqrt{2})^{-1}$, then

$$2^{m-1} - ((\ln 2)/2)^{\frac{1}{2}} 2^{m(1+H(r/m))/2} \lesssim \rho(r, m) \lesssim 2^{m-1} - (\sqrt{2}+1)^{r-1} 2^{(m-2)/2};$$

If $r/m = \frac{1}{2}$, then

$$n/4 \geq \rho(m/2, m) \geq H^{-1}(\tfrac{1}{2})n \approx 0.11n,$$

i.e., $\rho(m/2, m) = \theta(n)$.

Acknowledgement

We thank A. Tietävainen for mentioning the problem and for helpful discussions.

Appendix: Proof of formula (9)

We will show by induction that for $m \geqslant (\sqrt{2}+2)r$ the following inequality holds:

$$\rho(r, m) \leqslant 2^{m-1} - \frac{1}{(\sqrt{2}-1)^{r-1}} 2^{(m-2)/2} + \binom{m}{r}.$$

Easy fact:

$$H\left(\frac{1}{\sqrt{2}+2}\right) = \frac{1}{2} + \frac{1}{\sqrt{2}+2}\log(\sqrt{2}+1).$$

Hence,

$$\binom{(\sqrt{2}+2)^r}{r} \geqslant \frac{2^{(\sqrt{2}+2)rH((\sqrt{2}+2)^{-1})}}{\sqrt{8(\sqrt{2}+2)r \cdot \frac{1}{\sqrt{2}+2} \cdot \frac{\sqrt{2}-1}{\sqrt{2}+2}}}$$

$$= \frac{1}{\sqrt{8r}} 2^{(\sqrt{2}+2)r(\frac{1}{2}+(\sqrt{2}+2)^{-1})\log(\sqrt{2}+1)}$$

$$= \frac{1}{\sqrt{8r}} 2^{(\sqrt{2}+2)r/2 + r\log(\sqrt{2}+1)};$$

$$\frac{1}{(\sqrt{2}-1)^{r-1}} 2^{(\sqrt{2}+2)r/2-1} = 2^{(r-1)\log(\sqrt{2}+1)+r(\sqrt{2}+2)/2-1}$$

$$= 2^{r\log(\sqrt{2}+1)+r(\sqrt{2}+2)/2-1-\log(\sqrt{2}+1)}$$

$$= \frac{1}{(\sqrt{2}+1)} 2^{r\log(\sqrt{2}+1)r(\sqrt{2}+2)/2}.$$

Furthermore,

$$\binom{\lceil(\sqrt{2}+2)r\rceil}{r} \geqslant \binom{(\sqrt{2}+2)r}{r} \cdot \frac{\binom{\lfloor(\sqrt{2}+2)r\rfloor}{r}}{\binom{\lceil(\sqrt{2}+2)r\rceil}{r}}$$

$$\geqslant \binom{(\sqrt{2}+2)r}{r} \cdot \frac{\binom{(\sqrt{2}+2)r-1}{r}}{\binom{\lceil(\sqrt{2}+2)r\rceil}{r}}$$

$$= \binom{(\sqrt{2}+2)r}{r} \cdot \frac{(\sqrt{2}+1)r+1}{(\sqrt{2}+2)r} > \frac{1}{\sqrt{2}}\binom{(\sqrt{2}+2)r}{r},$$

$$\frac{1}{(\sqrt{2}-1)^{r-1}} 2^{\lceil(\sqrt{2}+2)r\rceil/2-1} < \frac{1}{\sqrt{2}(\sqrt{2}+1)} 2^{r\log(\sqrt{2}+1)+r(\sqrt{2}+2)/2}.$$

Thus,

$$\rho(r, \lceil(\sqrt{2}+2)r\rceil) \leqslant 2^{m-1} - \frac{1}{\sqrt{2}(\sqrt{2}+1)} 2^{r\log(\sqrt{2}+1)+r(\sqrt{2}+2)/2}$$

$$+ \frac{r}{4\sqrt{r}} 2^{r\log(\sqrt{2}+1)+r(\sqrt{2}+2)/2}$$

and for $r^{\frac{1}{2}}/4 > 1/(\sqrt{2}(\sqrt{2}+1))$, or for $r \geqslant 2$, we have $\rho(r, \lceil(\sqrt{2}+2)r\rceil) \leqslant 2^{m-1} + \varepsilon$, $\varepsilon > 0$, which is always valid since $\rho(r, m) < 2^{m-1}$ for $m \geqslant r$, and $r \geqslant 1$. Furthermore, $\lceil(\sqrt{2}+2)(r+1)\rceil - \lceil(\sqrt{2}+2)r\rceil \geqslant 3$.

The inequality (9) holds for $r = 2$ and all m. Let it be valid for some $r-1$ and all $m \geqslant \lceil(\sqrt{2}+2)(r-1)\rceil$. We will prove it for r and $m \geqslant \lceil(\sqrt{2}+2)r\rceil$. It is O.K. for $m = \lceil(\sqrt{2}+2)r\rceil$, thus for $m > \lceil(\sqrt{2}+2)r\rceil$ we have (note that $\lceil(\sqrt{2}+2)(r-1)\rceil$ is less than $\lceil(\sqrt{2}+2)r\rceil$)

$$\rho(r, m) \leqslant 2^{m-2} - \frac{1}{(\sqrt{2}-1)^{r-1}} 2^{(m-3)/2} + r\binom{m-1}{r}$$

$$+ 2^{m-2} - \frac{1}{(\sqrt{2}-1)^{r-2}} 2^{(m-3)/2} + (r-1)\binom{m-1}{r-1}$$

$$\leqslant 2^{m-1} - \frac{1}{(\sqrt{2}-1)^{r-1}} 2^{(m-2)/2} + r\binom{m}{r}. \qquad \square$$

References

[1] G.D. Cohen, M. Karpovsky, H. Mattson and J. Schatz, Covering radius, survey and recent results, IEEE Trans. Inform. Theory 31 (3) (1985) 328–343.

[2] A. McLoughlin, The covering radius of the $(m-3)$rd order Reed–Muller codes and a lower bound on the $(m-4)$th order Reed–Muller codes, SIAM J. Appl. Math. 37 (1979) 419–422.
[3] J.H. van Lint, Coding Theory, Lecture Notes in Math., Vol. 201 (Springer, Berlin, 1973).
[4] A. Tietäväinen, Covering radius and dual distance, Designs, Codes Cryptography (1991) 31–46.
[5] P. Solé, Asymptotic bounds on the covering radius of binary codes, IEEE Trans. Inform. Theory 36 (6) (1990) 1470–1472.